WEB APPLICATION FIREWALL

FortiWeb Release Notes

VERSION 6.0.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 12, 2018

FortiWeb 6.0.0 Release Notes

1st Edition

Change log

05/23/2018	Initial release.
06/12/2018	First update, adding the following new features or enhancements: • Iotop integration • "Traced By User" filter • GUI option to enable Auto Learn • New console command "`no-ssl-encrypt-then-mac: disable`" • New console command "`cert-config cert-config`"

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 6.0.0, build 0007.

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and zero-day threats. The Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep your applications safe from:

- Sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, and cookie poisoning
- Malicious sources
- DoS attacks

For additional documentation, please visit the FortiWeb documentation:

http://docs.fortinet.com/fortiweb/

What's new

FortiWeb 6.0 offers the following new feature and enhancements.

New Features

AI-based machine learning threat detection

FortiWeb now offers AI-based machine learning threat detection that replaces the existing auto-learn function. With this new capability, you can deploy FortiWeb to protect against known threats and zero-day attacks with few or virtually no false positives.

For more information about Machine Leaning and Auto Learn in 6.0, see "Change and performance notices" on page 10

Support for MAPI over HTTP

With support for publishing Exchange transport protocol MAPI, FortiWeb now can not only detect Trojans and scan email attachments using its integrated Anti-virus mechanism, but also forward files to FortiSandbox for additional scanning.

Addition of CVE IDs in attack logs and FortiView

A CVE ID column has been added to the attack log and the FortiView Server Policy tab. It makes it possible to report, track, and filter CVEs triggered by attack signatures.

Addition of Server Policy tab under FortiView

A new Server Policies tab has been added under FortiView>Security, enabling you to view data specific to a server policy. In the existing 6.0.0 release, only CVE IDs are viewable in this tab. Other views will be added in future releases

Support for Google Cloud

You can now run FortiWeb on the Google Cloud platform.

Support for VirtualBox—Oracle virtual platform

FortiWeb can now run on VirtualBox, the Oracle virtual platform.

Additions to the "execute" command

Two new console commands (see below) have been added to allow you to fix logdisk errors using fsck and remount the logdisk when it's lost.

```
execute fscklogdisk
execute remountgdisk
```

New console command option for "no-ssl-encrypt-then-mac"

```
FortiWeb # config server-policy setting
FortiWeb (setting) # get
hsm : disable
dpdk : disable
high-compatibility-mode: enable
fast-forward : disable
enable-core-file : enable
core-file-count : 3
offline-session-timeout: 120
enable-session-statistics: enable
enable-single-worker: disable
use-first-ack-mac : enable
no-session-limit : disable
no-ssl-encrypt-then-mac: disable
```

New console command for backing up and restoring certificates

```
FortiWeb # execute backup
   cert-config cert-config
   cli-config cli-config
   full-config fullconfig
```

Iotop integration

The integration enables you to easily debug the top input and out (I/O) processes currently running on the system.

Feature Enhancements

HTTP Header length increase

The maximum HTTP header length can be increased to 20 KB (CLI only).

Domain name in RADIUS server configuration

You can now configure a RADIUS server using its domain name.

Account takeover protection for user credential brute force

A new Predefined Advanced Protection rule has been added to protect against user credential brute force attacks. It is based on a new occurrence filter type "Tracked By User".

The rule monitors attempts that use multiple attacking sources on the same user name to overcome the existing brute force protections. *You must enable user tracking to use this feature.*

HTTP Protocol Constraints addition

A new HTTP protocol constraints rule has been added, enabling FortiWeb to detect Odd and Even Space Attacks.

Max character limit raised in signature exceptions

The maximum number of characters used in regex configuration for signature exceptions has been increased from 254 to 2048.

HA

You can make dynamic changes to Layer-2 HA configurations, and modify the MTU of the HA port to support HA in VXLAN environments

DHCP

Static and policy routes are now maintained during a FortiWeb upgrade or reboot.

Change and performance notices

Auto Learn in 6.0

With the introduction of machine learning behavior-based threat detection, we are retiring the auto-learn functionality. For new installations, Auto Learn is disabled and can be enabled by selecting **System>Config>Feature Visibility.** For existing installations, Auto Learn is enabled and visible in the left-side menu of the GUI. However, we recommend that you disable Auto Learn in policies and start using Machine Learning.

If you have ADOM enabled, make sure you enable Machine Learning in the access profile for the administrators you want to grant permissions to configure machine-learning policies.

For performance considerations, we do not recommend enabling both Auto Learn and Machine Learning in the same policy though it is possible to do so.

Machine Learning support in HA deployments

In version 6.0.0, no machine-learning policy or data is synced between HA nodes. For Active/Passive deployments, machine-learning policies are not synced to the standby node. In case of a failover, the standby node will therefore not have any machine-learning policies enabled. When the active node resumes standard operations, it will use the data it had before failing over.

For Active/Active deployments, machine learning is not supported. While you can still enable machine learning, machine-learning policies are not synced across the nodes. As a result, machine learning will only work on one node. This can lead to unexpected problems.

Enhancements to machine learning in HA deployments will be provided in future releases.

Supported deployment types when using Machine Learning

In version 6.0.0, machine learning is only supported in Reverse Proxy and True Transparent Proxy (TTP) deployments.

Disk partitioning requirement

To support the latest features and enhancements, your FortiWeb needs to be re-partitioned when you upgrade from any version prior to FortiWeb 5.5.

For instructions, see "Repartitioning the hard disk" on page 13.

Server health checks need to be reconfigured when upgrading to 5.9.x

The HTTP host header name for a health check has been moved from the health check configuration to the server pool configuration, and has been renamed from **Host** to **Health Check Domain Name** in the web UI. Because of this, when upgrading to 5.9.x, health checks will no longer work. To reconfigure a health check after upgrading to 5.9.x, enter the HTTP host header name for the health check in the relevant server pool configuration.

HTTP content routing is partially supported when HTTP/2 is enabled

When FortiWeb is deployed in Reverse Proxy mode and HTTP/2 is enabled, HTTP content routing is partially supported. FortiWeb can communicate with clients via HTTP/2, but FortiWeb should communicate with the server or server pool via HTTP. For example, if the **Deployment Mode** is `HTTP Content Routing` and **HTTP/2** is enabled, FortiWeb will negotiate HTTP/2 with clients during the SSL handshake, but the corresponding server pool in an HTTP content routing policy should still use HTTP.

HTTP content routing policies that match X.509 certificate content

In 5.5 Patch 4, the HTTP content routing policy settings that match X.509 certificate content were enhanced to allow you to match values found in either the client certificate's subject field or the extension field. When you upgrade from an earlier release, the upgrade process deletes any HTTP content routing policies that match X.509 certificate content. You can re-create these policies using the enhanced settings.

Log feature after upgrade

The logging feature does not work after you downgrade your FortiWeb 5.5 or later appliance to an earlier version and then upgrade back to the original version.

Software support for FortiWeb 400B and 1000B

FortiWeb 5.4 and later software is not supported on the 400B and 1000B platforms. Fortinet will continue to provide bug fixes to these models with 5.3.X patch releases.

Traffic logs

Very frequent disk writing may cause abnormal disk wear and tear and performance decreases. Fortinet recommends enabling traffic logs only when debugging problems. Disable traffic logs once FortiWeb is operating normally.

Failure to disable traffic logging during normal use may cause premature hard disk failure.

Time required to display data analytics reports

Depending on how much data must be analyzed for a query, data analytics queries can take some time. You should try filtering queries to include data from short periods of time.

Data analytics data set limitations

Due to the large amount of data that can be stored in the data analytics database, data analytics queries can search only up to 1,000,000 records at a time. This will be enhanced in later versions of FortiWeb.

Rebuilding the log aggregation database

In some cases, if the log aggregation database is damaged, the web UI does not display logs correctly on the **Aggregated Attacks** page. For example, duplicate logs may be displayed, or logs may be missing.

To correct these problems, use the following command to rebuild the database:

```
execute db rebuild
```

This operation does not delete any logs. For details, see the *FortiWeb CLI Reference*:

http://docs.fortinet.com/fortiweb/reference

Upgrade instructions

Hardware & VM support

FortiWeb 6.0.0 supports:

- FortiWeb 100D
- FortiWeb 400C
- FortiWeb 400D
- FortiWeb 600D
- FortiWeb 1000D
- FortiWeb 1000E
- FortiWeb 2000E
- FortiWeb 3000C/3000CFsx
- FortiWeb 3000D/3000DFsx
- FortiWeb 3000E
- FortiWeb 3010E
- FortiWeb 4000C
- FortiWeb 4000D
- FortiWeb 4000E
- FortiWeb-VM

Repartitioning the hard disk

To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb operating system's disk.

In most cases, you'll have to install a special firmware image to repartition the disk. For details, see "To use the special firmware image to repartition the operating system's disk " on page 14.

For the following FortiWeb-VM tools, you cannot install the special firmware image to repartition the hard disk:

- Citrix XenServer
- Open-source Xen Project
- Microsoft Hyper-V
- KVM

For these platforms, to repartition the disk you must deploy a new virtual machine and restore the configuration and log data you backed up earlier. See "To repartition the operating system's disk without the special firmware image" on page 14.

Repartitioning affects the operating system's disk (USB/flash disk), not the hard disk. Existing data such as reports and event, traffic, and attack logs, which are on the hard disk, are not affected.

You can use this image to upgrade an HA cluster by following the same procedure you use for a regular firmware upgrade. For details, see "Updating firmware on an HA pair" in the *FortiWeb Administration Guide*:

http://docs.fortinet.com/fortiweb/admin-guides

To use the special firmware image to repartition the operating system's disk

1. Perform a complete backup of your FortiWeb configuration.

   Although the repartitioning firmware image automatically saves your FortiWeb configuration, Fortinet recommends that you also manually back it up. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides

2. Go to the Fortinet Customer Service & Support website to download the special repartitioning firmware image from the FTP site:

   https://support.fortinet.com/

   Ensure that you download the correct image for your FortiWeb platform.

3. Follow one of the same procedures that you use to install or upgrade firmware using a standard image:

   - In the Web UI, go to **System > Status > Status**. Locate the **System Information** widget. Beside **Firmware Version**, click **[Update]**.
   - In the Web UI, go to **System > Maintenance > Backup & Restore**. Select the **Restore** option in **System Configuration**.
   - In the CLI, enter the `execute restore config` command.

   FortiWeb backs up the current configuration, resizes the hard drive partitions, and boots the system.

4. Continue with the instructions in "Upgrading from previous releases" on page 16.

To repartition the operating system's disk without the special firmware image

1. Perform a complete backup of your FortiWeb configuration. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides

2. Use the instructions for your hypervisor platform to detach the log disk from the VM:

   - "To detach the log disk from a Citrix XenServer VM" on page 15
   - "To detach the log disk from a Microsoft Hyper-V VM" on page 15
   - "To detach the log disk from a KVM VM" on page 15

3. Deploy a new FortiWeb 5.5 or later virtual machine on the same platform.

4. Use the instructions for your hypervisor platform to attach the log disk you detached earlier to the new VM:

- "To attach the log disk to a Citrix XenServer VM" on page 15
- "To attach the log disk to a Microsoft Hyper-V VM" on page 15
- "To attach the log disk to a KVM VM" on page 16

5. Restore the configuration you backed up earlier to the new VM.
6. When you are sure that the new VM is working properly with the required configuration and log data, delete the old VM.

To detach the log disk from a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the VM, on the Storage tab, select **Hard disk 2**, and then click **Properties**.
3. For **Description**, enter a new description, and then click **OK**.
4. Select **Hard disk 2** again, and then click **Detach**.
5. Click **Yes** to confirm the detach task.

To detach the log disk from a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the FortiWeb-VM in the list of machines, and then, under **Actions**, click **Settings**.
2. Select **Hard Drive (data.vhd)**, and then click **Remove**.
3. Click **Apply**.

To detach the log disk from a KVM VM

1. In Virtual Machine Manager, double-click the FortiWeb-VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.

To attach the log disk to a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the new, FortiWeb 5.5 or later VM, on the Storage tab, select **Hard disk 2**, and then click **Delete**.
3. Click **Yes** to confirm the deletion.
4. On the Storage tab, click **Attach Disk**.
5. Navigate to the hard disk you detached from the old VM to attach it.
6. Start your new virtual machine.

To attach the log disk to a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the new, FortiWeb 5.5 or later virtual machine in the list of machines, and then, under Actions, click **Settings**.
2. Select **Hard Drive (log.vhd)**, and then click **Browse**.

3. Browse to the hard drive you detached from the old virtual machine to select it.
4. Click **Apply**.
5. Start the new virtual machine.

To attach the log disk to a KVM VM

For KVM deployments, you remove an existing virtual disk from the new VM before you attach the disk detached from the original VM.

1. In Virtual Machine Manager, double-click the new, FortiWeb 5.5 or later VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.
4. Click **Add Hardware**.
5. Click **Storage**, select **Select managed or other existing storage**, and then click **Browse**.
6. Click **Browse Local**.
7. Navigate to the log disk file for the original machine to select it, and then click **Open**.
8. For **Device type**, select **Virtio disk**, for **Storage format**, select **qcow2**, and then click **Finish**.
9. Start the new virtual machine.

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

To download the Customer Service & Support image checksum tool

After logging in to the website, in the menus at the top of the page, click **Download**, and then click **Firmware Image Checksums**.

Alternatively, near the bottom of the page, click the **Firmware Image Checksums** button. This button appears only if one or more of your devices has a current support contract. In the **File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from previous releases

- To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb hard disk partitions. See "Repartitioning the hard disk" on page 13.

- If you upgrade from a version of FortiWeb previous to 5.5.4, the upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.
- If you upgrade from a version of FortiWeb previous to 5.3.6, the upgrade process deletes any V-zone IP addresses, which are no longer required. This operation has no impact on routing or connectivity after the upgrade.
- If you upgrade from a version of FortiWeb previous to 5.3.4 and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.

Note: To upgrade from 4.0 MR4, Patch x or earlier, please contact Fortinet Technical Support.

To upgrade from FortiWeb 5.5.x

Upgrade to FortiWeb 6.0.0 directly.

To upgrade from FortiWeb 5.4.x or FortiWeb 5.3.x

Upgrade to FortiWeb 6.0.0 directly after completing the hard disk repartitioning process.

If you are upgrading FortiWeb-VM on a hypervisor other than VMware vSphere, see "FortiWeb-VM license validation after upgrade from pre-5.4 version" on page 18.

To upgrade from a version previous to FortiWeb 5.3

FWB5.3.exe is a Microsoft Windows executable script that automatically migrates your FortiWeb 5.2.x configuration settings to a 5.3.x configuration.

1. If your version is 5.0.x or 5.1.x, upgrade to FortiWeb 5.2.x.
2. Use **System > Maintenance > Backup & Restore** to back up your FortiWeb configuration. Fortinet recommends that you use the **Backup entire** configuration option.

   Note: If you forget to back up the configuration before you upgrade to FortiWeb 5.3, you can use the **Boot into alternate firmware** option to downgrade to the previous version, and then backup its configuration. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides
3. To obtain the upgrade script, log in to the Fortinet Customer Service & Support website:

   https://support.fortinet.com

   In the menus at the top of the page, click **Download**, and then click **Firmware Images**.
4. For product, select **FortiWeb**. Then, on the Download tab, navigate to the following folder:

   `/FortiWeb/v5.00/5.3/Upgrade_script/`
5. Download the .zip compressed archive (for example, `FWB5.3Upgrade_v1.9.zip`) to a location you can access from your Windows PC.
6. In Windows, extract the .zip archive's contents, and then use a command line interface to execute the upgrade script.

   For example, in the directory where the file `FWB5.3Upgrade.exe` and your backup configuration file are located, execute the following command:

```
FWB5.3Upgrade.exe -i YOUR_CONFIG_NAME.conf -o 5.3_new.conf
```

The script removes the Domain Server, Physical Server, Server Farm, Content Routing policy configurations and generates a new configuration file named `5.3_new.conf`.

7. Resize your FortiWeb hard disk partitions. See "Repartitioning the hard disk" on page 13.
8. Upgrade to FortiWeb 6.0.0.
9. Use **System > Maintenance > Backup & Restore** to restore the configuration file you created using the script (for example, `5.3_new.conf`).

   If you upgrade from a previous version of FortiWeb and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.

Upgrading an HA cluster

If the HA cluster is running FortiWeb 4.0 MR4 or later, the HA cluster upgrade is streamlined. When you upgrade the active appliance, it automatically upgrades any standby appliance(s), too; no manual intervention is required to upgrade the other appliance(s). This includes upgrading using the special hard disk repartitioning firmware image for upgrading to 5.5 or later from earlier releases.

If the HA cluster is running FortiWeb 4.0 MR3 Patch x or earlier, contact Fortinet Technical Support for assistance.

Downgrading to a previous release

When you downgrade your FortiWeb 6.0.0 to version 5.1 or 5.0, the basic configuration for your appliance's connections to the network (e.g., IP address and route configuration) is preserved.

FortiWeb-VM license validation after upgrade from pre-5.4 version

On some virtual machine deployments, upgrading FortiWeb-VM from a version previous to 5.4 changes the virtual machine's universal unique identifier (UUID). Because of this change, the first time you upload your existing FortiWeb-VM license, the FortiGuard Distribution Network (FDN) server reports that it is invalid.

To solve this problem, after you have uploaded the license, wait 90 minutes, and then upload the license again.

This issue does not affect FortiWeb-VM deployed on a VMware vSphere hypervisor.

Resolved issues

This section lists issues that have been fixed in version 6.0.0. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
0475874	After losing connection for a while, sandboxd would get killed by OOM.
0479855	FortiWeb HA mode cannot run heartbeat on FortiGate VXLAN.
0487343	Inconsistent use of quotation marks in log fields caused interpretation issues to the Syslog/SIEM server.
0489275	Three translation errors were found on the GUI of the Japanese version.
0488713	A slave unit in an HA configuration could leave the group, resulting in a split-brain situation.
0489514	The secondary FortiWeb in an HA cluster could automatically remove the group-ID, causing a split-brain situation due to configuration sync failure from the Console.
0482923	Once logged in through CAPTCHA, the page would display an "ERR_EMPTY_RESPONSE" error upon refresh.
0415766	Alert emails were sent whenever they were triggered instead of at the interval set in email policy.
0484892	Disk logging could stop all of a sudden, with disk space utilization reaching to around 90%.
0483962	The log filter would not work with a user name containing a backslash "\".
0479178	Static routes could get lost during FortWeb upgrade.
0483783	Errors on the console of the slave unit could cause the slave unit to disconnect from the HA cluster.

Known issues

This section lists known issues in version 6.0.0, but may not be a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
0483785	The SFP Transreciever on Fortiweb Finisar FTLF8519P3BNL does not come up on FortiWeb 600D.
0488993	The TSL CA could not be restored using the "`restore cert-config`" command.
0488811	The HSM certificate could not be restored using the "`restore cert-config`" command.
0490315	The limit on health check buffer size could cause inaccurate health check information to be displayed.
0478579	This bug applies to only FortiWeb-VM on XenServer: In a High Availability deployment, if the primary and standby appliances switch roles, you can't access the pserver afterwards.
0471903	In a signature rule, if the **Action** for the **Information Disclosure** option is set to `Alert & Erase`, the attack log message ID that FortiWeb generates in response to a rule violation will contain the erased information.
0475874	If FortiWeb loses the connection with FortiSandbox, sandboxd may crash due to an `out of memory` error.
0479855	In a High Availability deployment, FortiWeb cannot run a heartbeat on FortiGate VXLAN.
0490792	When you execute the `formatlogdisk` command several times upon upgrading from v583, the console would print an MySQL- related error.
0490732	In an AWS HA environment, it would take a while for the main device to get the license; the standby device wan unable to obtain the license.